AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0020.1] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes an x86-compatible microprocessor. The x86-compatible microprocessor has an instruction register having a single, atomic cryptographic instruction disposed therein, a keygen unit, and an execution unit. ~~The instruction register is within the x86-compatible microprocessor and has a single, atomic cryptographic instruction disposed therein. The single, atomic cryptographic instruction is part of an application program, and the x86-compatible microprocessor executes the application program.~~ The single, atomic cryptographic instruction prescribes ~~an encryption operation, is arranged according to the instruction format for execution on the x86-compatible microprocessor, and also prescribes~~ that a user-generated key schedule be employed when executing ~~the encryption~~an encryption operation. The encryption operation that is prescribed by the single, atomic cryptographic instruction comprises encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks. The keygen unit is operatively coupled to the instruction register. The keygen unit directs the x86-compatible microprocessor to load the user-generated key schedule. The execution unit is operatively coupled to the keygen unit. The execution unit employs the user-generated key schedule to execute the encryption operation. The execution unit includes a cryptography unit that is configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, where the plurality of cryptographic rounds are prescribed by a control word that is provided to the cryptography unit. The cryptography unit executes a first plurality of micro instructions

generated by translation of the single, atomic cryptographic instruction. The execution unit also includes an x86 integer unit, an x86 floating point unit, an x86 MMX unit, and an x86 SSE unit, where the cryptography unit operates in parallel with the x86 integer unit, the x86 floating point unit, the x86 MMX unit, and the x86 SSE unit, to accomplish the encryption operation, where the x86 integer unit executes a second plurality of micro instructions generated by the translation to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of the plurality of cryptographic rounds.

[0021] One aspect of the present invention contemplates an apparatus for performing cryptographic operations. The apparatus has a cryptography unit within a x86-compatible microprocessor; an x86 integer unit, an x86 floating point unit, an x86 MMX unit, and an x86 SSE unit, each of the units also disposed within the x86-compatible microprocessor; and a keygen unit. The cryptography unit executes a decryption operation responsive to receipt of a single, atomic cryptographic instruction within an application program that prescribes the decryption ~~operation , where the single, atomic cryptographic instruction is arranged according to the instruction format for execution on the x86-compatible microprocessor, and where the x86-compatible microprocessor executes the application program~~. The single, atomic cryptographic instruction also prescribes that a user-generated key schedule be employed when executing the decryption operation . The decryption operation that is prescribed by the single, atomic cryptographic instruction comprises decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks, where the cryptography unit executes a first plurality of micro instructions generated by translation of the single, atomic cryptographic instruction. The cryptography unit operates in parallel with the x86 integer unit, the x86 floating point unit, the x86 MMX unit, and the x86 SSE unit, to accomplish the decryption operation, where the x86 integer unit executes a second plurality of micro instructions generated by the translation to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of the plurality of cryptographic rounds. The keygen unit is operatively coupled to the cryptography unit. The keygen unit directs the x86-compatible microprocessor to perform the

decryption operation and to employ the user-generated key schedule when performing the decryption operation.

[0022] Another aspect of the present invention provides a method for performing cryptographic operations in a x86-compatible microprocessor. The method includes executing an application program that is stored in memory, where the executing includes receiving a single, atomic cryptographic instruction from the memory that prescribes employment of a user-generated key schedule during execution of an encryption operation within a cryptographic unit in the x86-compatible microprocessor, and where the encryption operation that is executed responsive to the single, atomic cryptographic instruction comprises ~~encryption of~~execution of a plurality of cryptographic rounds on a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks;. ~~The single, atomic cryptographic instruction is arranged according to the instruction format for execution on the x86-compatible microprocessor.~~ The ~~method~~ executing also includes ~~employing the user-generated key schedule when executing the encryption operation to generate a result of the encryption operation,~~ within a cryptographic unit in the x86-compatible microprocessor, employing the user-generated key schedule when executing the encryption operation to generate a result of the encryption operation, wherein the cryptographic unit executes a first plurality of micro instructions generated by translation of the single, atomic cryptographic instruction. The executing further includes, within an integer unit in the x86-compatible microprocessor, executing a second plurality of micro instructions generated by the translation to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of the plurality of cryptographic rounds.